

CLAIMS

1. A method for managing a network connection in a network configuration comprising a firewall, said method comprising:

- a. automatically determining whether said network connection is active; and
- b. deleting a state of said network connection if said network connection is not active.

2. The method of claim 1, wherein said automatically determining whether said network connection is active comprises:

- a1. generating a probe, said probe causing a network activity corresponding to said network connection; and
- a2. sensing said network activity to determine whether said network connection is active.

3. The method of claim 2, wherein said firewall comprises a database for storing information relating a state of said network connection and wherein, in response to said network activity, said firewall updates information stored in said database.

4. The method of claim 3, wherein said stored information comprises an idle time counter of said network connection and wherein said firewall resets said time counter if said network connection is determined to be active.

5. The method of claim 2, wherein said network connection is between a client and a server and said probe comprises a packet containing probe data, and wherein said probe data is a copy of first data, said first data having been sent by the server and received and acknowledged by said client during preceding communication between said client and said server.

6. The method of claim 5, wherein said network activity comprises a response from said client indicating a condition of said network connection.

7. The method of claim 6, wherein said response of said client comprises a data receipt acknowledgment if said network connection is active and an error message if said network connection is not active.

8. The method of claim 2, wherein said probe is nondestructive with respect to said network connection.

9. The method of claim 2, wherein said probe is generated by said firewall.

10. A computer readable medium embodying a program for managing a network connection in a network configuration comprising a firewall, said program comprising:

- a. automatically determining whether said network connection is active; and
- b. deleting a state of said network connection if said network connection is not active.

11. The computer readable medium of claim 10, wherein said automatically determining whether said network connection is active comprises:

a1. generating a probe, said probe causing a network activity corresponding to said network connection; and

a2. sensing said network activity to determine whether said network connection is active.

12. The computer readable medium of claim 11, wherein said firewall comprises a database for storing information relating a state of said network connection and wherein, in response to said network activity, said firewall updates information stored in said database.

13. The computer readable medium of claim 12, wherein said stored information comprises an idle time counter of said network connection and wherein said firewall resets said time counter if said network connection is determined to be active.

14. The computer readable medium of claim 11, wherein said network connection is between a client and a server and said probe comprises a packet containing probe data, and wherein said probe data is a copy of first data, said first data having been sent by the server and received and acknowledged by said client during preceding communication between said client and said server.

15. The computer readable medium of claim 14, wherein said network activity comprises a response from said client indicating a condition of said network connection.

16. The computer readable medium of claim 15, wherein said response of said client comprises a data receipt acknowledgment if said network connection is active and an error message if said network connection is not active.

17. The computer readable medium of claim 11, wherein said probe is nondestructive with respect to said network connection.

18. The computer readable medium of claim 11, wherein said probe is generated by said firewall.

19. A firewall configured for managing a network connection, wherein said firewall automatically determines whether said network connection is active and deletes a state of said network connection if said network connection is not active.

20. The firewall of claim 19, wherein said firewall generates a probe, said probe causing a network activity corresponding to said network connection; and senses said network activity to determine whether said network connection is active.

21. The firewall of claim 20, wherein said firewall comprises a database for storing

SUN REF.: P5374 US

information relating a state of said network connection and wherein, in response to said network activity, said firewall updates information stored in said database.

22. The firewall of claim 21, wherein said stored information comprises an idle time counter of said network connection and wherein said firewall resets said time counter if said network connection is determined to be active.

23. The firewall of claim 20, wherein said network connection is between a client and a server and said probe comprises a packet containing probe data, and wherein said probe data is a copy of first data, said first data having been sent by the server and received and acknowledged by said client during preceding communication between said client and said server.

24. The firewall of claim 23, wherein said network activity comprises a response from said client indicating a condition of said network connection.

25. The firewall of claim 24, wherein said response of said client comprises a data receipt acknowledgment if said network connection is active and an error message if said network connection is not active.

26. The firewall of claim 20, wherein said probe is nondestructive with respect to said network connection.

27. The firewall of claim 20, wherein said probe is generated by said firewall.

28. A computer system comprising at least a central processing unit and a memory, said memory storing a program for managing a network connection in a network configuration comprising a firewall, said program comprising:

- a. automatically determining whether said network connection is active; and
- b. deleting a state of said network connection if said network connection is not active.

29. The computer system of claim 28, wherein said automatically determining whether said network connection is active comprises:

- a1. generating a probe, said probe causing a network activity corresponding to said network connection; and
- a2. sensing said network activity to determine whether said network connection is active.

30. The computer system of claim 29, wherein said firewall comprises a database for storing information relating a state of said network connection and wherein, in response to said network activity, said firewall updates information stored in said database.

31. The computer system of claim 30, wherein said stored information comprises an idle time counter of said network connection and wherein said firewall resets said time counter if

said network connection is determined to be active.

32. The computer system of claim 29, wherein said network connection is between a client and a server and said probe comprises a packet containing probe data, and wherein said probe data is a copy of first data, said first data having been sent by the server and received and acknowledged by said client during preceding communication between said client and said server.

33. The computer system of claim 32, wherein said network activity comprises a response from said client indicating a condition of said network connection.

34. The computer system of claim 33, wherein said response of said client comprises a data receipt acknowledgment if said network connection is active and an error message if said network connection is not active.

35. The computer system of claim 29, wherein said probe is nondestructive with respect to said network connection.

36. The computer system of claim 29, wherein said probe is generated by said firewall.